The Impact of Rational Party in Multiparty Computation and the Counteracts

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy

BY
Dhaneshwar Mardi
Reg. No. NITD/PhD/IT/2016/00804

Under the Supervision
of
Dr. Jaydeep Howlader
Department of Computer Science and Engineering



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY DURGAPUR
WEST BENGAL -713209
INDIA

September, 2022

Abstract

Multiparty computation allows $n \geq 2$ parties to compute a publicly known function on their private inputs. The goal of multiparty computation is to compute the function correctly while parties learn only the output of the function, yet no party learns any additional information about the input of other parties. Multiparty computation inherently defines that parties are curious to learn other's input, but the system does not allow them to do so. Generally, multiparty computation assumes that some parties (a set of parties) are distrustful and either deviates from the protocol or form a coalition. There are two categories of parties: honest and faulty. The honest party always follows the protocol without any deviation. On the other hand, a faulty party either deviates from the protocol or colludes.

Game Theory, on the other hand, analyzes the interaction among the parties in a strategic environment where the entities are rational and intelligently. Here parties play simultaneously and independently. Unlike the competitive game where the winner defeats others, the objective of the parties in a strategic game is to maximize their payoff (or utility). Rationality implies that each party chooses the strategy to maximize his payoff irrespective of the other party's payoff. Intelligence implies that the party always selects the best strategy among all possibilities. The objective of the game is to reach equilibrium conditions.

There are certain scenarios where multiparty computation and game theory share the common goal of interests. Specifically, the parties are induced to behave rationally by incentivizing at the end-result. In this case, parties always intend to achieve certain results, eventually maximizing their incentives.

In this dissertation, we investigate the impact of rational parties on multiparty computation. The public function of multiparty computation is considered a strategic game. Generally, the dominant strategy guarantees risk-neutral and maximizes the players' utility. However, the dominant strategy may indulge social imbalance and

compromise individual input privacy. Therefore, we re-investigated the game with incentive-compatibility and ensured the participants' truthful behavior. We design some mechanisms (or rules) to impose the incentive-compatibility.

We have also investigated the class of functionalities that multiparty computation can compute. Specifically, we have raised the question - whether multiparty computation computes all the functionaries that a trusted third party computes. Our investigation reveals that all regular language functionalities (which require finite memory), are computable using multiparty computation.

Finally, we present an implementation of incentive-compatibility mechanism in the Bitcoin anonymous protocol. Bitcoins inherently have some degree of anonymity. The identity of the Bitcoin owner is a pseudonym. Therefore, one can trace back along the *blockchain* to find the owner of the coin. Our proposed anonymous bitcoin protocol applies multiparty computation and guarantees truthful behavior of the owners who like to make their coins anonymous. Instead of a pseudonym, we have used a mixing mechanism to make the output unlinkable.